МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2011
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2011
Proceedings of the Fortieth Jubilee Spring Conference
of the Union of Bulgarian Mathematicians
Borovetz, April 5–9, 2011

THE CLOUD COMPUTING AND COMPUTER VIROLOGY

Eugene Nickolov, Dimitrina Polimirova

The paper presents the current situation of “cloud computing” and “cloud information attacks” in the light of computer virology and information security. The categories“cloud possible information attacks” and “cloud successful information attacks” are discussed. The architecture of “cloud computing” and the main components that make up its infrastructure – “clients”, “datacenters” and “dirstributed servers” are commented. The services offered by the “cloud computing” as SaaS, HaaS and PaaS are also commented. The advantages and disadvantages of the components and services with respect to the “cloud information attacks” are pointed. An analysis of the current situation of “cloud information attacks” at the area of Bulgaria, Balkan Peninsula and Sought-East Europe with respect to the components and services is made. The results are presented as 3D graphical objects. At the end in the part of conclusion the assessments and recommendations are presented.

1. Introduction. The evolution of modern computer and communication systems, which remains constant over the past 40 years reached its peak to present dates in the form of ”cloud computing”. The expenditures of designing and manufacturing integrated circuits which are the base of modern information systems have reached a limit beyond which the need for real, much more funds became critical important.

The global financial and economic crisis increased the lack of funds emphatically. Therefore, creating the present and looking to the future the computer companies sharply increased the funding of this type of services that have become popular in recent years as cloud services.

These services are implemented through the construction of real computer systems that are virtualized, i.e. 3–4 virtual computer systems based on a real computer system are created. Thus, creating computing resources that repeatedly exceed the current computing needs appears a significant surplus of computing resources. Accumulating and organizing this computing surplus in the form of public free or corporation paid service, the big computer companies created new market niche with huge sizes as an increased reliance they used the established historical allegory ”cloud” as a substitute for Internet and that way this surplus of computing resources have “brought up” into the “clouds” as a undefined point in the coordinate system, which summarizes in itself the global concept The Net.

In this respect all the existing problems of ”ground” computer systems with respect to the security proved to be also ”brought up” in the ”clouds”.

The computer viruses and the science that deals with them – the computer virology – received its new development, received its new direction of research and its new philosophy to ensure the protection on the user level, on the application level, on the system level and on the network level.

The aim of this paper is to present in a relatively concise and understandable way the main existing directions of information attacks, accomplished within the cloud environment.

Analysis of known techniques for successful implementation of an information attack in the cloud environment is made. An assessment of the main advantages and disadvantages of the methods of protection in cloud computing is given.

For the analysis and evaluation the characteristics of architecture of the cloud and of the individual customers, through which services in the cloud environment are accessible will be taken into account.

Cloud information attacks could be divided into *possible* and *successful* information attacks. As *possible* information attacks we understand those attacks whose mechanism of action allows operation, i.e. "bringing up" in the "cloud" and as *successful* information attacks we understand those attacks whose presence can be documented in the cloud and there is an evidence of completing its mission (executed scenario).

2. Cloud architecture and cloud components. The **architecture** of the cloud involves the use of combinations of hardware and software related in a unified whole, which is designed for a specific set of activities of so-called architect of cloud computing. This means a lot of cloud components to carry out dependent activities among themselves through the Application Program Interface (API) such as web services.

The main **components** in building of cloud environment are so-called clients. Through them, most often using the browser the cloud architecture provides access to the services. In addition to the mentioned above clients the following additional components – datacenters and distributed servers should be selected when creating a global cloud computing implementation. The mutual location in hierarchical levels and relationships between them defines the general topology of the cloud computing implementation (Figure 1).

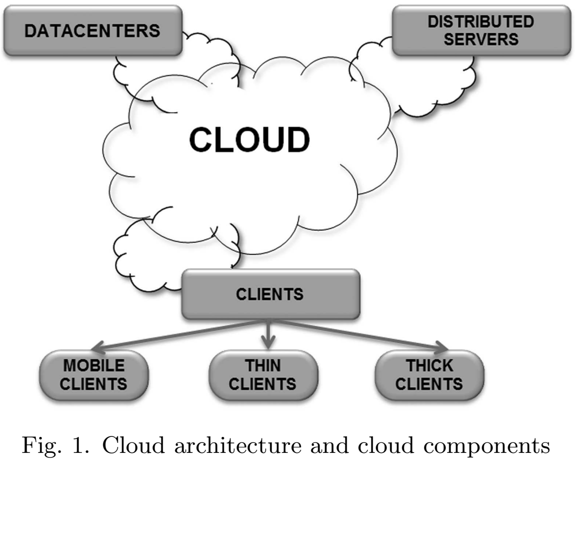


Fig. 1. Cloud architecture and cloud components

The **clients** can be presented as desktop workstations, mobile workstations, Personal Digital Assistants (PDAs), tablets, notebooks, netbooks, smartphones, etc. The clients can be also divided into: *mobile clients, thin clients* and *thick clients* [1].

The *mobile clients* include PDA's family, MS PocketPC's family, iPhone's family, iPad's family, Blackberry's family, etc.

The *thin clients* are built on personal computers which don't have embedded memory devices such as HDD or SSD. The thin clients receive information directly from the server which after reaction of the user the information is returned to the server. They are relatively cheap and reliable solution when working with server virtualization.

The *thick clients* are built on standard desktop computers, which are connected to the cloud via web browser. The thick clients also receive the information directly from the server, but they process substantial amount of information locally on their own resources after that they return the information back to the server.

The **datacenters** are built on certain grouping and accordingly natural focusing of the servers, which have regard to the application/applications which are used in the cloud [2]. Their physical location may be within an adjacent building, a neighboring town, a neighboring country or a neighboring continent. It should be noted that on the real servers a certain amount of virtual servers that may exceed the actual number of real servers by 30 times to date are created.

The **distributed servers** are also built on real servers, but in that case the concentrating of the servers on one place is missing [3]. This means that parts of our application can be processed/located on a given server/servers in South America, another part of the application – on the territory of North America, a third part – on the territory of Australia, while our client is in Europe.

3. Cloud services. The power of attraction of cloud computing is in the possibility just to put our "cable" on and to receive our service.

Now there are three main types of cloud services:

- Software as a Service (SaaS) [3];
- Hardware as a Srvice (HaaS) [4];
- Platform as a Service (PaaS) [5].

It is of a great significance to note that we are "tenants" of the services offered by the cloud.

The **Software as a Service** is based on the hypothesis that an application is hosted as a service in the cloud and the users can use it via Internet. In this case the user has no obligation about supporting the software. Additionally, he has no obligation about settings and/or supporting the integration of the application with other systems. The service provider guarantees the operating state of the cloud. Examples of such applications are CRM systems, CMS systems, etc.

The **Hardware as a Service** is based on the hypothesis that we are able to rent CPU time, computer memory, network equipment, computer peripherals, etc. The supplier ensures that resources are available, effective and economical. Obligation of the supplier is to provide an optimal strategy of using with respect to the time and with respect to the expenses, even in cases when several tenants rent together hardware resources to reduce their expenses.

The **Platform as a Service** is based on the hypothesis that the tenant/tenants of the cloud absolutely commit all resources necessary for building applications and providing services entirely in Internet without needing to download and install any software on the local clients. Design tools, building tools, testing tools and hosting of applications can be included in it. Additionally possibilities for integration with other services, integration with local or remote databases, etc. can be included.

4. The current situation of cloud information attacks. The existence of cloud computing is inextricably bound up with the cloud information attacks.

This is because the special nature of cloud computing doesn't eliminate the existence of information attacks. They continue to exist, to implement their planned scenarios and to consume their tangible advantages. Only their name which reflects the change of their working environment is changed.

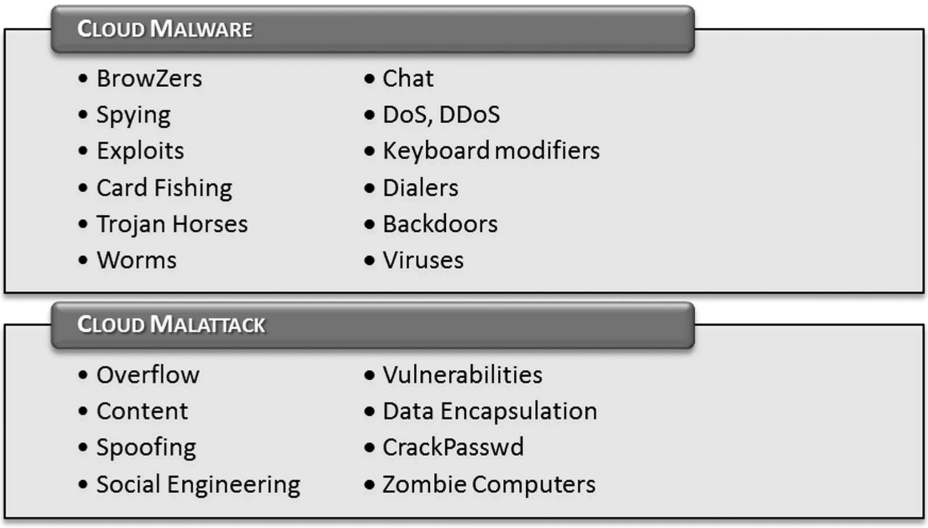
In this paper an information from the information database of National Laboratory of Computer Virology – BAS is used which includes the information attacks, accomplished to and into cloud environment on the territory of Bulgaria, Balkan Peninsula and South-East Europe for the period 2009–2010 [6].

Cloud information attacks include the categories *cloud possible information attacks* and *cloud successful information attacks.*

The diversity of cloud information attacks, accomplished for the last two years is impressive. Generally they can be divided into two main groups:

- cloud malware (cloud malicious software, which operates fully automatically without the presence of a user during the execution of the scenario);
- cloud malattacks (cloud malicious attacks, which don't operate fully automatically and they suppose presence of a user during the execution of the scenario).

In the category of *cloud possible information attacks* are included 20 main types attack tools, respectively: 12 types of cloud malware and 8 types of cloud malattacks (Figure 2).



CLOUD MALWARE

- BrowZers
- Spying
- Exploits
- Card Fishing
- Trojan Horses
- Worms
- Chat
- DoS, DDoS
- Keyboard modifiers
- Dialers
- Backdoors
- Viruses

CLOUD MALATTACK

- Overflow
- Content
- Spoofing
- Social Engineering
- Vulnerabilities
- Data Encapsulation
- CrackPasswd
- Zombie Computers

Fig. 2. Main groups and types *cloud possible information attacks*

In the category of *cloud successful information attacks* are included 20 main types attack tools, respectively: 8 types of cloud malware and 4 types of cloud malattacks (Figure 3).

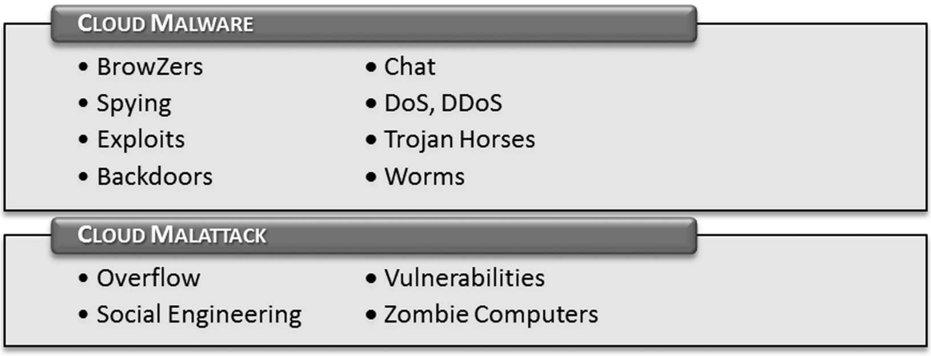


Fig. 3. Main groups and types *cloud successful information attacks*

4.1. Comparative analysis of cloud information attacks with respect to the cloud components. The prospects for development of cloud computing should be evaluated by appropriate analysis throughout the depth of the problem. At first it means to evaluate the impact of single components on the cloud information attacks. We do it by indicating their advantages and disadvantages with respect to the cloud information attacks.

The advantage of **mobile clients** is that a relatively limited number of attacks can be accomplished through them to the clouds, because they are relatively new and there are no accumulated knowledge in the relevant volumes. Their disadvantage is primarily the lack of comparatively powerful solutions for the information security, because this target market is yet to develop.

The advantage of **thin clients** is that they have relatively few resources and that means relatively possibilities for attacks. Their disadvantage is in the fact that any protection loads additional the resources, and this is not desirable due to requirements for dimensions, price and power consumption.

The advantage of **thick clients** is that they are fully equipped work places and the protection can be realized completely. Their disadvantage is in the fact that having available significant resources significantly more potentially dangerous actions are accomplished.

The advantage of **datacenters** is in the fact that when concentrating in one point of the relatively hardware and software resources, high level of competence for protection from attacks is achieved easier. Their disadvantage is in the big amount of available resources that means that the protection from attack is much more difficult and significantly more expensive.

The advantage of **distributed servers** is that they are territorially scattered and possible attacks will not be able to easily cover them all. Their disadvantage is in their communication loss and relatively delays of information flows which could be delayed more because a protection against the attacks will be needed to apply.

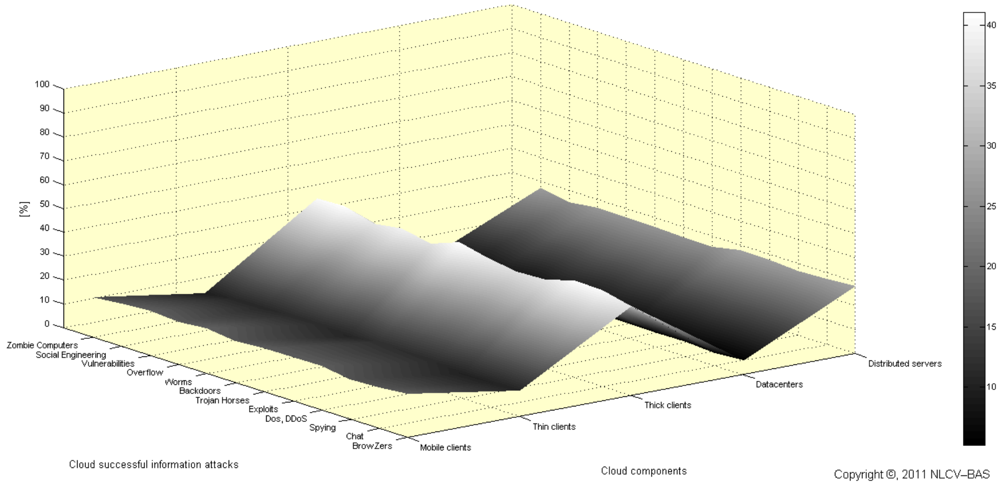


Fig. 4. Percentage distribution of *cloud successful information attacks* accomplished to cloud components

Figure 4 shows the percentage distribution of *cloud successful information attacks* accomplished to *cloud components.*

4.2. Comparative analysis of cloud information attacks with respect to the cloud services. The advantage of **Software as a Service** is that its flexibility

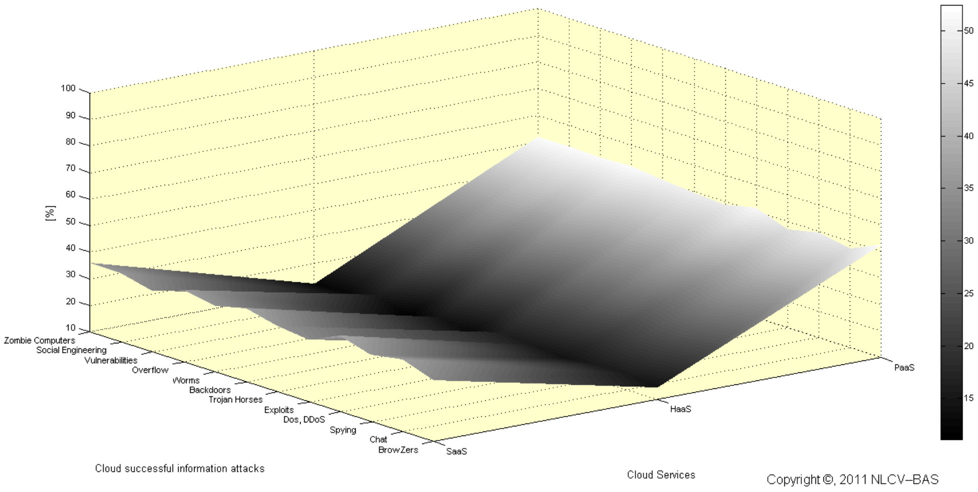


Fig. 5. Percentage distribution of *cloud successful information attacks* accomplished to cloud services

supposes opportunity for founded vulnerabilities and omissions to be repaired in the next versions of the software after update. Its disadvantage is in its insufficient protection by tenants of the service when high loading.

The advantage of **Hardware as a Service** is that HaaS is relatively resistant to cloud attacks because the significant part of configuration settings are stored as unvarying factory records. Its disadvantage is in its relative inability to eliminate founded vulnerabilities.

The advantage of **Platform as a Service** is that PaaS offers completely full service with appropriate protection with respect to the cloud attacks on a high corporate level. Its disadvantage is in the fact that the price is comparatively high and its requirements to the tenants are comparatively high.

Figure 5 shows the percentage distribution of *cloud successful information attacks* accomplished to cloud services.

5. Conclusion. The future of cloud information structures looks promising!

The future of cloud information attacks also looks promising!

The natural fear of the consumers for their own data and investments will prevent the rapid penetration of cloud computing. Restraint will be also the relatively low level of information security which is result of relatively high success of cloud information attacks.

The predictions which can be made include seriously expansion of cloud computing in the near future. They are suitable for all, and for providers and for tenants.

REFERENCES

[1] T. Velte, A. Velte, T. J. Velte, R. Elsenpeter. Cloud Computing: A Practical Approach. McGraw Hill Professional, 2009, p. 7, ISBN 0071626948.

[2] T. Tronco. New Network Architectures: The Path to the Future Internet. Studies in Computational Intelligence, vol **297**, Springer, 2010, 179–186, ISBN 3642132464.

[3] H. Spaanenburg, L. Spaanenburg. Cloud Connectivity and Embedded Sensory Systems. Springer, 2010, p. 30, p. 33, ISBN 1441975446.

[4] W. Chang, H. Abu-Amara, J. Sanford. Transforming Enterprise Cloud Services. Springer, 2010, 98–100, ISBN 9048198453.

[5] B. Furht, A. Escalante. Handbook of Cloud Computing. Springer, 2010, 343–346, ISBN 1441965238.

[6] National Cybersecurity Portal (`http://ncs.nlcv.bas.bg/index.htm`)

Eugene Nickolov, Dimitrina Polimirova
National Laboratory of Computer Virology
Bulgarian Academy of Sciences
Acad. G. Bonchev Str., Bl 8
1113 Sofia, Bulgaria
e-mail: eugene.nickolov@nlcv.bas.bg
polimira@nlcv.bas.bg

“ОБЛАЧНИ ИЗЧИСЛЕНИЯ” И КОМПЮТЪРНА ВИРУСОЛОГИЯ

Евгений Николов, Димитрина Полимирова

Докладът представя текущото състояние на “облачните изчисления” и “облачните информационни атаки” в светлината на компютърната вирусология и информационната сигурност. Обсъдени са категориите “облачни възможни информационни атаки” и “облачни успешни информационни атаки”. Коментирана е архитектурата на “облачните изчисления” и основните компоненти, които изграждат тяхната инфраструктура, съответно “клиенти” (“clients”), „центрове за съхранение на данни“ (“datacenters”) и „разпределени сървъри“ (“dirstributed servers”). Коментирани са и услугите, които се предлагат от “облачните изчисления” – SaaS, HaaS и PaaS. Посочени са предимствата и недостатъците на компонентите и услугите по отношение на “облачните информационни атаки”. Направен е анализ на текущото състояние на “облачните информационни атаки” на територията на България, Балканския полуостров и Югоизточна Европа по отношение на компонентите и на услугите. Резултатите са представени под формата на 3D графични обекти. На края са направени съответните изводи и препоръки под формата на заключение.